(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－8617

(43)公開日　平成11年(1999)１月12日

(51)Int.Cl.[6]		識別記号	FI		
H04L	9/12		H04L	9/00	631
G06F	13/00	351	G06F	13/00	351G
G09C	1/00	660	G09C	1/00	660E
H04L	9/32		H04L	9/00	673B
	12/54			11/20	101B

審査請求　有　請求項の数３　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願平9－160989

(22)出願日　平成９年(1997)６月18日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　佐藤　太郎
東京都港区芝五丁目７番１号　日本電気株式会社内

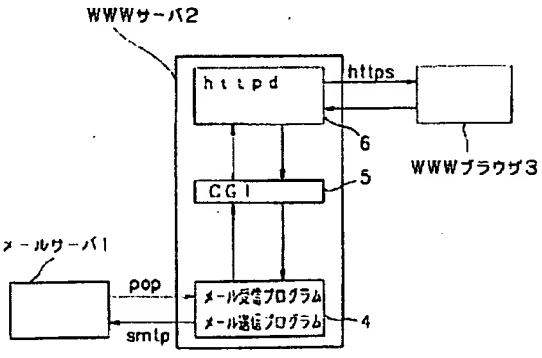
(74)代理人　弁理士　丸山　隆夫

(54)【発明の名称】　電子メールの暗号化システム及び暗号化方法

(57)【要約】

【課題】　電子メールの送受信を安全に行い、かつ、効率的に行うことの可能な電子メールの暗号化システム及び暗号化方法を提供する。

【解決手段】　少なくとも１以上の端末に備えられたＷＷＷブラウザ３が、電子メールをｈｔｔｐｓにより暗号化して送信し、かつ、受信したｈｔｔｐｓにより暗号化された電子メールを復号化して画面に表示させ、メールサーバ１が、受信した電子メールを蓄積し、ＷＷＷサーバ２が、端末から送信されたｈｔｔｐｓにより暗号化された電子メールを復号化してメールサーバ１に送信し、かつ、メールサーバ１から送信された電子メールをｈｔｔｐｓにより暗号化してＷＷＷブラウザ３が備えられた端末に送信する。



【特許請求の範囲】

【請求項１】　電子メールをｈｔｔｐｓにより暗号化して送信し、かつ、受信したｈｔｔｐｓにより暗号化された電子メールを復号化して画面に表示させるWWWブラウザを備えた少なくとも１以上の端末と、

受信した電子メールを蓄積するメールサーバと、

前記端末から送信されたｈｔｔｐｓにより暗号化された電子メールを復号化して前記メールサーバに送信し、かつ、前記メールサーバから送信された電子メールをｈｔｔｐｓにより暗号化して前記端末に送信するWWWサーバとを有することを特徴とする電子メールの暗号化システム。

【請求項２】　前記WWWサーバが、

前記端末から送信されたｈｔｔｐｓにより暗号化された電子メールを復号化し、かつ、電子メールをｈｔｔｐｓにより暗号化して出力するｈｔｔｐｄと、前記ｈｔｔｐｄにより復号化された電子メールをメールサーバに送信すると共に、前記メールサーバから送信された電子メールを受信するＣｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅとを有することを特徴とする請求項１記載の電子メールの暗号化システム。

【請求項３】　端末に備えられたWWWブラウザにより、電子メールをｈｔｔｐｓにより暗号化してWWWサーバに備えられたｈｔｔｐｄに送信する工程と、

前記暗号化された電子メールをWWWサーバに備えられたｈｔｔｐｄにより復号化し、Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅに送信する工程と、

前記Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅに送信された電子メールを、Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅに備えられたメール送信プログラムに従ってメールサーバに送信する工程とを備えた、端末からメールサーバへの電子メール送信工程と、

前記Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅが、ＣｏｍｍｏｎＧａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅに備えられたメール受信プログラムに従ってメールサーバから電子メールを受信し、該受信した電子メールを前記ｈｔｔｐｄに出力する工程と、

前記ｈｔｔｐｄが、ｈｔｔｐｄに出力された電子メールを、ｈｔｔｐｓにより暗号化してWWWブラウザが備えられた端末に送信する工程と、

前記暗号化された電子メールを受信した端末が、前記WWWブラウザにより受信した電子メールを復号化して表示する工程とを備えた、メールサーバから端末への電子メール送信工程とを有することを特徴とする電子メールの暗号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子メールの暗号化システム及び暗号化方法に関し、特に端末に備えられたWWWブラウザにより電子メールを送受信する場合の電子メールの暗号化システム及び暗号化方法に関する。

【０００２】

【従来の技術】現在、インターネットの発展に伴い、そのネットワークにおいて取り扱われるデータに対するセキュリティの向上が重要な課題となっている。

【０００３】特に、Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ（以下、単にWWWと記す。）上での電子メール送受信方式は、メールサーバに電子メールを蓄積することができ、利用者の都合に合わせて電子メールの送受信を行えるため、その簡便さから広く利用され、それに伴い、電子メールを取り扱う際の、秘密保持やデータの複製防止等のセキュリティの向上が必要となっている。

【０００４】そのため、従来では、電子メールを暗号化して送受信を行う方式が提案されている。

【０００５】従来、この種の電子メールを暗号化しての送受信は、電子メールの内容を、送信者及び受信者以外の第三者に読まれることを防ぐために用いられている場合が多い。

【０００６】例えば、電子メールの暗号化送受信方法の一例として、特開平８－２５１１５６号公報に開示された、「電子メール暗号化方法及び暗号化システム」について、以下に説明する。

【０００７】この公報に記載された電子メールの暗号化送受信方法は、通信ネットワークの各利用者のそれぞれが、各々の鍵情報を作成し、公開鍵を公開することによって暗号化を可能にし、セキュリティの向上を図るものである。

【０００８】具体的には、前準備として各利用者が各々の鍵情報を専用のソフトウェアで作成し、あらかじめセンタに登録しておく。送信する電子メールを暗号化する際は、電子メール本文をデータ鍵により暗号化し、このデータ鍵をマスタ鍵により暗号化し、この２つの暗号化されたデータを電子メールデータとして送信する。この２つの暗号化されたデータを受信した端末は、暗号化されたデータ鍵のデータをマスタ鍵を用いて復号化し、この復号化されたデータ鍵を用いて暗号化された電子メールデータを復号化し、電子メールの受信を行う。

【０００９】従って、この従来の電子メールの暗号化送受信方法によれば、電子メールの偽造や複製等を有効に防止し、安全性の高い電子メール暗号化方法を提供することができるとしている。

【００１０】

【発明が解決しようとする課題】しかしながら、上述の従来の電子メールの暗号化送受信方法においては、送受信を行う端末を特定し、この特定された端末間で鍵を共有する必要があるため、個々の端末において鍵情報を作成し、かつ、この鍵情報を公開しなければならず、電子メールの暗号化を行う際の効率が低減すると共に、ネットワークの安全性にも支障をきたすという問題点を有する。

【００１１】また、上述のような従来の電子メールの暗号化システムにおいては、電子メールの暗号化及び復号化を、個々の端末上において実行しているため、個々の端末は、それぞれ暗号化及び復号化のためのハードウェアやソフトウェア等を具備しなければならず、暗号化及び復号化を行うためのその端末のコストが上昇するという問題点を有する。

【００１２】本発明は、上記事情に鑑みなされたもので、電子メールの送受信を安全に行い、かつ、効率的に行うことの可能な電子メールの暗号化システム及び暗号化方法を提供することを目的とする。

【００１３】

【課題を解決するための手段】請求項１記載の発明は、電子メールをｈｔｔｐｓにより暗号化して送信し、かつ、受信したｈｔｔｐｓにより暗号化された電子メールを復号化して画面に表示させるWWWブラウザを備えた少なくとも１以上の端末と、受信した電子メールを蓄積するメールサーバと、前記端末から送信されたｈｔｔｐｓにより暗号化された電子メールを復号化して前記メールサーバに送信し、かつ、前記メールサーバから送信された電子メールをｈｔｔｐｓにより暗号化して前記端末に送信するWWWサーバとを有することを特徴とする。

【００１４】従って、この発明によれば、端末とメールサーバとの間において電子メールの送受信を行う場合、WWWサーバと端末との間においては、その電子メールが、ｈｙｐｅｒ　ｔｅｘｔ　ｔｒａｎｓｆｅｒ　ｐｒｏｔｏｃｏｌ（以下、単にｈｔｔｐと記す。）におけるセキュリティ強化型のプロトコルである、ｈｔｔｐｓにより暗号化されていることから、安全に電子メールの送受信を行うことができる。

【００１５】また、電子メールを暗号化する際には、WWWサーバ及びWWWブラウザがｈｔｔｐｓによる暗号化を行うので、個々の端末の鍵情報の作成や、その公開等は必要ではないので、電子メールの暗号化の効率を向上させることができ、その安全性を向上させることができる。

【００１６】また、端末に備えられたWWWブラウザにより電子メールに対する暗号化及び復号化を行って送受信を行うため、電子メールを暗号化及び復号化して送受信する際に新たな部材を設ける必要はない。

【００１７】また、端末の利用者はWWWサーバからｈｔｔｐｓにより暗号化され転送された電子メールの内容をWWWブラウザが備えられた端末の画面において読むことができ、逆にWWWブラウザが備えられた端末の画面で記入した電子メールの内容をｈｔｔｐｓにより暗号化してWWWサーバに転送することができるので、ｈｔｔｐｓにより暗号化された電子メールの送受信は、インターネット上の任意の場所の端末において行うことができる。

【００１８】請求項２記載の発明は、請求項１記載の発明において、前記WWWサーバが、前記端末から送信されたｈｔｔｐｓにより暗号化された電子メールを復号化し、かつ、電子メールをｈｔｔｐｓにより暗号化して出力するｈｔｔｐｄと、前記ｈｔｔｐｄにより復号化された電子メールをメールサーバに送信すると共に、前記メールサーバから送信された電子メールを受信するＣｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅとを有することを特徴とする。

【００１９】従って、この発明によれば、請求項１記載の発明の作用が得られると共に、電子メールの暗号化及び復号化をWWWサーバに備えられた、ｈｔｔｐサーバである、ｈｔｔｐｄ（ｈｙｐｅｒ　ｔｅｘｔ　ｔｒａｎｓｆｅｒ　ｐｒｏｔｏｃｏｌｄｅｍｏｎ）が行ない、メールサーバとの間での電子メールの送受信をＣｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅ（以下、ＣＧＩと言う。）が行い、同様に、端末では、端末に備えられたWWWブラウザが電子メールの暗号化及び復号化を行っているため、暗号化及び復号化を行うためのｈｔｔｐｓに対応したWWWブラウザであれば電子メールの暗号化及び復号化を行えるため、特別な部材を用いることなく電子メールの暗号化及び復号化を行うことができる。

【００２０】請求項３記載の発明は、端末に備えられたWWWブラウザにより、電子メールをｈｔｔｐｓにより暗号化してWWWサーバに備えられたｈｔｔｐｄに送信する工程と、前記暗号化された電子メールをWWWサーバに備えられたｈｔｔｐｄにより復号化し、Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅに送信する工程と、前記Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅに送信された電子メールを、Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅに備えられたメール送信プログラムに従ってメールサーバに送信する工程とを備えた、端末からメールサーバへの電子メール送信工程と、前記Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅが、Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅに備えられたメール受信プログラムに従ってメールサーバから電子メールを受信し、該受信した電子メールを前記ｈｔｔｐｄに出力する工程と、前記ｈｔｔｐｄが、ｈｔｔｐｄに出力された電子メールを、ｈｔｔｐｓにより暗号化してWWWブラウザが備えられた端末に送信する工程と、前記暗号化された電子メールを受信した端末が、前記WWWブラウザにより受信した電子メールを復号化して表示する工程とを備えた、メールサーバから端末への電子メール送信工程とを有することを特徴とする。

【００２１】従って、この発明によれば、端末からメールサーバへ電子メールを送信する場合は、端末に備えられたWWWブラウザにより電子メールをｈｔｔｐｓにより暗号化してWWWサーバに送信し、WWWサーバに備えられたｈｔｔｐｄはこの電子メールを復号化し、Ｃｏ

mmon Gateway Interfaceがこの復号化された電子メールをメール送信プログラムに基づいてメールサーバに送信し、また、メールサーバから端末への電子メールを送信する場合には、Common Gateway Interfaceがメール受信プログラムに基づいてメールサーバから電子メールを受信し、この受信した電子メールをhttpdに送信し、httpdがこの送信された電子メールをhttpsにより暗号化してWWWブラウザに送信するので、従来技術のように、電子メールの暗号化及び復号化を行う際に、個々の端末において鍵情報を作成するという手間を省くことができると共に、その鍵情報を公開する必要もないため、その安全性を向上することができる。

【００２２】また、電子メールの暗号化及び復号化が、httpsにより行われているため、一般的なWWWブラウザであれば電子メールの暗号化及び復号化を行うことができ、電子メールの暗号化及び復号化のための特別な部材を必要としないので、電子メールの暗号化及び復号化を行う際のコストの上昇を抑えることができる。

【００２３】

【発明の実施の形態】次に、本発明に係る電子メールの暗号化システム及び暗号化方法の実施形態について図面を参照して詳細に説明する。

【００２４】図１に、本発明に係る電子メールの暗号化システムの一実施形態の構成の概念図を示す。この図１に示されるように、この電子メールの暗号化システムは、受信した電子メールを蓄積するメールサーバ１と、メールサーバ１から電子メールを受信し、WWWブラウザ３からhttpsにより暗号化された電子メールを受信するWWWサーバ２と、メールサーバ１に送受信する電子メールを表示するためのWWWブラウザ３とから構成されている。

【００２５】また、上述のWWWサーバ２は、メール受信プログラム及びメール送信プログラム４を有するCGI（Common Gateway Interface）５と、CGI５との間で電子メールの送受信を行い、WWWブラウザ３との間でhttpsにより暗号化された電子メールの送受信を行うhttpd６とから構成される。ここで、以下に述べるhttpsは、Open Systems Interconnection（開放型システム間相互接続）におけるSecurity Socket Layer（以下、単にSSLと記す。）を用いる。

【００２６】WWWサーバ２に備えられているhttpd６は、一般に広く用いられているhttps（SSL）を利用可能なものであるならば、どのような種類のものを用いても良い。また、通常の方法でhttpsにより、WWWブラウザ３との間において暗号化通信を行う。

【００２７】WWWブラウザ３は市販されているhttps（SSL）対応のものであるならばいずれでも良く、またインターネット上の特定の場所の端末に備えられている必要はない。従って、WWWブラウザ３はhttpd６と通信することが可能な任意の場所の端末にあれば良い。

【００２８】メールサーバ１はWWWサーバ２と同一のコンピューター上にあり、その機能は一般に広く用いられているUNIX（登録商標）のsendmailと何ら変わるところはない。すなわち、メールサーバ１には、電子メールの暗号化のための特別な部材を付与する必要はない。

【００２９】次に、この図１を参照して、本発明に係る電子メールの暗号化方法について説明する。

【００３０】WWWブラウザ３から、メールサーバ１に蓄積された電子メール講読の要求がhttpd６に送られると、httpd６は、CGI５が有するメール受信プログラム４にメール受信要求を出力する。

【００３１】メール受信要求を受けたメール受信プログラム４は、メールサーバ１にメール受信要求を出力する。メール受信要求を受けたメールサーバ１は、要求された電子メールをCGI５に送信する。そして、CGI５に備えられたメール受信プログラム４は、通常のpopプロトコルにより電子メールを受信する。この受信した電子メールをCGI５がhttpd６に出力する。

【００３２】httpd６は電子メールをhtml（hyper text mark－up language）に成形した上で、httpsにより暗号化してWWWブラウザ３に送信する。

【００３３】一方、WWWブラウザ３から電子メールの送信データがhttpd６に送られる場合、送信される電子メールはWWWブラウザ３とhttpd６との間において、httpsにより暗号化されて転送される。

【００３４】httpd６はこの送信された電子メールをCGI５を介してメール送信プログラム４に出力する。電子メールを受信したメール送信プログラム４は、通常のsmptプロトコルにより電子メールをメールサーバ１に送信する。

【００３５】従って、この電子メールの暗号化方法によれば、WWWブラウザ３とhttpd６との間における電子メールの送受信が、httpsにより暗号化された電子メールを用いて行われているため、ネットワーク上における電子メールの秘密保持を適切に行えると共に、暗号化を行う際に、端末に暗号化のための特別な部材を設ける必要が無いため、端末のコストの上昇を抑えることができる。

【００３６】次に、図１に示される電子メールの暗号化システムにおけるWWWブラウザ３の画面表示の一例を図２を参照して説明する。

【００３７】図２に、図１に示されるWWWブラウザ３による画面表示の一例を示す。ただし、図１に示す電子

メールの暗号化システムと同様な部材には同じ番号を付す。この図２に示されるように、WWWブラウザ３からWWWサーバ２にアクセスし、電子メール送受信用のパスワード入力画面２１をWWWブラウザ３に表示する。この画面にはＣＧＩに備えられた送受信用のプログラムとやり取りする項目が記述されている。ここでメールサーバ１のユーザー名とパスワードを入力すると、図１に示されるＣＧＩ５の制御により、電子メール受送信選択の画面２３が表示される。

【００３８】電子メール受信を選択すると、電子メール一覧の画面２５が表示され、メールサーバ１に届いている電子メールのタイトルの一覧を見ることができる。この画面で閲覧したい電子メールのタイトルを選択すると、電子メール受信・閲覧の画面２７においてメールの内容を見ることができる。

【００３９】受送信選択の画面で電子メール送信を選択すると、電子メール送信の画面２９が表示され、電子メールを記入しWWWサーバ２に送信するための情報が入力できる。

【００４０】WWWサーバ２とWWWブラウザ３との間の通信はすべてｈｔｔｐｓにより暗号化されているので、画面に表示される情報、入力する情報は暗号化されてWWWサーバ２に届く。WWWサーバ２とメールサーバ１との間は通常のｐｏｐ、ｓｍｔｐによりデータが流れるが、メールサーバ１とｈｔｔｐｄ６とが同一のコンピューター上にあるため、電子メールがネットワーク上を流れることはなく、その安全性についての問題はない。

【００４１】従って、この電子メールの暗号化方法の一実施形態によれば、WWWブラウザ３を備えた端末が電子メールの受信を行う場合には、その受信する電子メールがｈｔｔｐｓにより暗号化され、さらに、WWWブラウザ３を備えた端末からメールサーバに電子メールの送信を行う場合には、WWWブラウザ３により暗号化されていることにより、その電子メールのセキュリティを向上させることができ、暗号化及び復号化における特別の部材も、各端末において必要ではないことから、端末のコストの上昇も抑えることができる。

【００４２】次に本発明に係る電子メールの暗号化システムの実施形態について図面を参照してさらに詳細に説明する。図３に、本発明に係る電子メールの暗号化システムの一実施形態の概略図を示す。

【００４３】この図３に示されるように、この電子メールの暗号化システムは、企業内ネットワーク（イントラネット）３９と、企業の外、つまり社外のネットワーク（インターネット）上の端末３７との間において電子メールをやり取りする場合を想定している。

【００４４】企業内ネットワーク３９は、受信した電子メールを蓄積するメールサーバ３１と、WWWサーバ３３と、外部からの不必要なデータの進入を阻止するｆｉｒｅｗａｌｌ３５とから構成されている。

【００４５】企業内ネットワーク３９はｆｉｒｅｗａｌｌ３５により守られており、従って、この内部での通常の電子メールの送受信は暗号化されていない。しかしながら社外のネットワークに電子メールのデータが流れるときは、暗号化を行う。

【００４６】この場合、ｆｉｒｅｗａｌｌ３５は、社外からWWWサーバ３３のみはアクセスできるように設定されている。このことにより、WWWサーバ３３と社外の端末３７とは通信を行える。

【００４７】WWWサーバ３３は市販のｈｔｔｐｓ（ＳＳＬ）を用いた暗号化サーバであり、社外の端末３７との間の通信は、すべてｈｔｔｐｓにより暗号化される。また、WWWサーバ３３にはメールサーバ３１との間で電子メールを送受信するＣＧＩプログラムが組み込まれている。

【００４８】この図３に示される電子メールの暗号化システムの動作について詳細に説明する。図３を参照すると、社外の端末３７からメールサーバ３１に蓄積されている電子メールを受信するためには、まず社外の端末３７に組み込まれているWWWブラウザ（不図示）を利用してWWWサーバ３３にアクセスする。

【００４９】WWWサーバ３３には電子メールを受信したことを示す画面があり、社外の端末３７上のWWWブラウザからメールサーバ３１のユーザ名およびパスワードを入力すればＣＧＩプログラムを介してメールサーバ３１上の電子メールが表示される。

【００５０】その際、メールサーバ３１とWWWサーバ３３との間は電子メールが暗号化されずに転送されるが、WWWサーバ３３と社外の端末３７との間はｈｔｔｐｓ（ＳＳＬ）により、暗号化されて転送される。

【００５１】逆に、社外の端末３７からメールサーバ３１に対して電子メールを送信する場合は、WWWサーバ３３の電子メール送信画面上に社外の端末３７のWWWブラウザから電子メールの内容を入力する。すると、WWWサーバ３３はＣＧＩプログラムを介して入力された電子メールをメールサーバ３１に送信する。この際、社外の端末３７からWWWサーバ３３までの間は、電子メールの内容はｈｔｔｐｓにより暗号化されて転送される。

【００５２】従って、この実施形態によれば、社外ネットワークに接続された社外の端末３７において、メールサーバ３１に蓄積された電子メールの送受信を行う場合、ｈｔｔｐｓにより暗号化された電子メールを用いて、WWWサーバ３３と社外の端末３７との間において電子メールのやり取りを行っているため、安全に電子メールの送受信を行うことができる。

【００５３】また、電子メールの暗号化及び復号化は、WWWサーバ３３、又は社外の端末３７に備えられたWWWブラウザにより行われており、特にWWWブラウザ

は、ｈｔｔｐｓに対応したものであるならば一般的なものを利用することができるため、電子メールを暗号化及び復号化するために特別な部材を特に設ける必要はないため、社外の端末３７のコストの上昇を抑えて電子メールの暗号化及び復号化を行うことができる。

【００５４】また、社外の端末３７は、ｈｔｔｐｓに対応したWWWブラウザを備えていれさえすれば良いため、社外ネットワーク上の任意の位置から、暗号化された電子メールの送受信を行うことができる。

【００５５】

【発明の効果】以上の説明から明らかなように、本発明によれば、Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂにおいて採用されているｈｔｔｐｓ（ＳＳＬ）という暗号化通信の技術を用いることにより、WWWサーバとWWWブラウザとの間の全ての通信におけるデータを暗号化しているため、送受信を行う個人の特定、若しくは端末の特定を行わずに、電子メールを暗号化して送受信でき、ネットワーク上の任意の場所から、専用のソフトウェアを用いずに暗号化された電子メールを送受信することができ、その安全性と、効率を向上することの可能な電子メールの暗号化システム及び暗号化方法を提供することができる。

【００５６】また、暗号化はWWWサーバとWWWブラウザ各々における情報とを使用して行うため、電子メールの暗号化のための個人、若しくは個々の端末の情報は不要である。そのため、鍵の公開等が不要であり、電子メールの暗号化を効率的に行うことが可能な電子メールの暗号化システム及び暗号化方法を提供することができる。

【図面の簡単な説明】

【図１】本発明に係る電子メールの暗号化システムの一実施形態の概念図である。

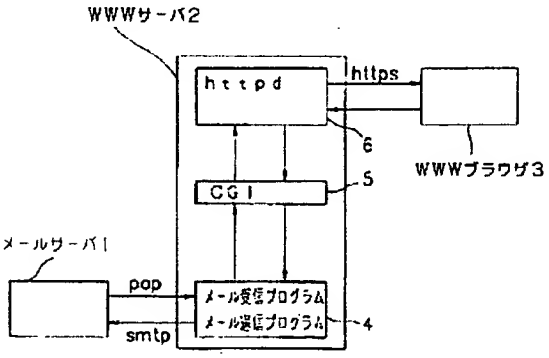
【図２】図１に示す電子メールの暗号化システムにおけるWWWブラウザによる表示画面の一例を示す図である。

【図３】本発明に係る電子メールの暗号化システムの一実施形態の概略図である。

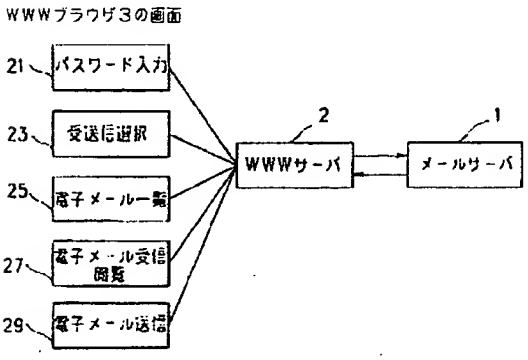
【符号の説明】

１　メールサーバ
２　WWWサーバ
３　WWWブラウザ
４　メール受信プログラム及びメール送信プログラム
５　ＣＧＩ（Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅ）
６　ｈｔｔｐｄ
２１　パスワード入力画面
２３　受送信選択画面
２５　電子メール一覧画面
２７　電子メール受信・閲覧画面
２９　電子メール送信画面
３１　メールサーバ
３３　WWWサーバ
３５　ｆｉｒｅｗａｌｌ
３７　社外の端末
３９　企業内ネットワーク

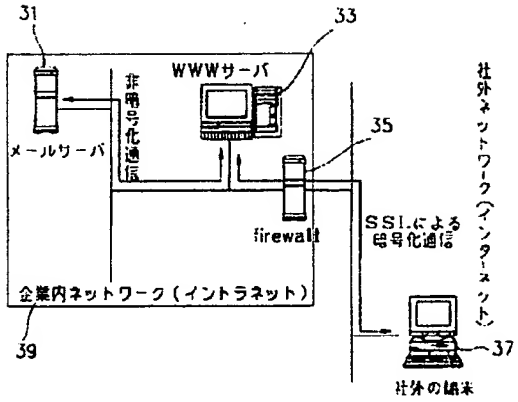
【図１】



【図２】



【図３】



フロントページの続き

(51) Int. Cl.[5]	識別記号	Ｆ Ｉ
Ｈ０４Ｌ　12/58		